JOHN A. YANCHUNIS (*pro hac vice*)
jyanchunis@forthepeople.com
JONATHAN B. COHEN (*pro hac vice*)
jcohen@forthepeople.com
RYAN J. McGEE (*pro hac vice*)
rmcgee@forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

Counsel for Plaintiffs Matt Matic and Zak Harris

Clayeo C. Arnold, SBN 65070
carnold@justice4you.com
Joshua H. Watson, SBN 238058
jwatson@justice4you.com
CLAYEO C. ARNOLD
A PROFESSIONAL LAW CORPORATION
865 Howe Avenue
Sacramento, California 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

IVY T. NGO, SBN 249860
ngoi@fdazar.com
FRANKLIN D. AZAR & ASSOCIATES, P.C.
14426 East Evans Avenue
Aurora, Colorado 80014
Telephone: (303) 757-3300
Facsimile: (720) 213-5131

Counsel for Plaintiffs Charles Olson and Eileen M. Pinkowski

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE GOOGLE PLUS PROFILE LITIGATION

Case No. 5:18-cv-06164-EJD (VKD)

CONSOLIDATED CLASS ACTION COMPLAINT

Judge: Hon. Edward J. Davila
Date Filed: October 8, 2018
Lead Counsel Hearing: March 23, 2019
Trial Date: None set

TABLE OF CONTENTS

For their Consolidated Class Action Complaint, Plaintiffs Matt Matic, Zak Harris, Charles Olson, and Eileen M. Pinkowski (collectively "Plaintiffs") on behalf of themselves and all others similarly situated, allege the following against Defendant Google LLC ("Google") and Alphabet Inc. ("Alphabet") (collectively, "Defendants"), based on personal knowledge as to Plaintiffs and Plaintiffs' own acts and on information and belief as to all other matters based upon, *inter alia*, the investigation conducted by and through Plaintiffs' undersigned counsel:

SUMMARY OF THE CASE

This case involves two related data leaks affecting millions of people who have used Defendants' Google+ social network. The first data leak, which Defendants knew about for months before announcing it on October 8, 2018, involves the improper exposure of the personal information of up to 500,000 Google+ users ("Google+ Users" or "Users") due to a software glitch that gave third-party application developers access to private Google+ profile data between 2015 and March 2018 (the "First Data Leak"). The second data leak, as Defendants disclosed just over two months later on December 10, 2018, similarly involves the improper exposure of the personal information of Users to third-party application developers, except this time, ***up to 52.5 million Users*** were affected (the "Second Data Leak"). These data leaks are collectively referred to herein as the "Google+ Data Leaks."

Launched in June 2011, Google+ (or Google Plus) is a social network owned and operated by Google for consumers with Google accounts. Google+ facilitates the sharing of information, photographs, weblinks, conversations, and other shared content similar in many respects to the Facebook news feed or Twitter stream. Google+ replaced Google's previous social network effort, Google Buzz, after the platform faced lawsuits and an action by the Federal Trade Commission ("FTC") concerning users' numerous privacy concerns with the platform, including alleged misrepresentations regarding Google's privacy assurances to users.

As part of the sign-up process and as a consequence of interacting with the network, Google+ Users create, maintain, and update profiles containing significant amounts of Personal Information, including their names, birthdates, hometowns, addresses, locations, interests,

relationships, email addresses, photos, and videos, amongst other information ("Personal Information").

Google maintains a privacy policy that makes specific representations to its users regarding its affirmative duty to protect users' Personal Information, specifically providing that users are in control of who has access to their Personal Information ("Privacy Policy").

When a User adds a contact to his or her Google+ account, the User assigns that person to one or more "circles" in order to categorize or organize the contact. Google+ Users determine privacy settings for content they share on Google+, allowing content to be shared with the public or with only those people in their designated circles.

While Users' Personal Information was supposed to be protected and shared only with their expressed permissions and limitations, Defendants allowed third-party application developers to improperly collect the Personal Information of up to 500,000 Google+ Users in the First Data Leak.

Instead of choosing to be transparent about the First Data Leak, Defendants explicitly chose to conceal it from the public until after the public outcry following Facebook's widely publicized Cambridge Analytica scandal had exhausted – hoping to avoid both public and Congressional scrutiny.

Then, just over two months after Defendants' announcement of the First Data Leak, Defendants announced the Second Data Leak, whereby the Personal Information of Users was, ***again***, improperly exposed to third-party applications developers. But this time, ***up to 52.5 million Users*** were impacted.

This Consolidated Class Action Complaint is filed on behalf of all persons in the United States, described more fully *infra*, whose Personal Information was compromised in the Google+ Data Leaks.

JURISDICTION AND VENUE

This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least

one class member is a citizen of a state different from Defendants. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

Venue is proper under 28 U.S.C. § 1391(c) because Defendants are corporations that do business in and are subject to personal jurisdiction in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claims in this action occurred in or emanated from this District, including the decisions made by Defendants' governance and management personnel that led to the Google+ Data Leaks and the decision not to disclose the First Data Leak earlier.

Further, the venue provision in Google's Terms of Service governing users in the United States provides an additional reason that venue is proper in this District. That provision provides for venue in the Northern District of California for all claims arising out of Plaintiffs' relationship with Google.

The Terms of Service also provide that all claims that might arise between Users and Defendants would be governed by the laws of California, without regard to conflict-of-law provisions. Accordingly, the choice-of-law provision establishes that California law applies to Plaintiffs' and the other Class members' claims.

PARTIES

A. Plaintiffs

Plaintiff Matt Matic is a resident and citizen of California. Plaintiff Matic opened a Google+ account and has used it for many years. Plaintiff Matic also uses a Gmail account for his primary email. Through the opening and use of these accounts, Plaintiff Matic has entrusted Google with his Personal Information for all relevant time periods.

Plaintiff Zak Harris is a resident and citizen of Florida. Plaintiff Harris opened a Google+ account and has used it since the inception of the platform. Plaintiff Harris also uses a Gmail account for email. Through the opening and use of these accounts, Plaintiff Harris has entrusted Google with his Personal Information for all relevant time periods.

Plaintiff Charles Olson is a resident and citizen of Colorado. Plaintiff Olson opened a Google+ account and has used it for at least four years. Plaintiff Olson also uses a Gmail account

for his primary email. Through the opening and use of these accounts, Plaintiff Olson has entrusted Google with his Personal Information for all relevant time periods.

Plaintiff Eileen M. Pinkowski is a resident and citizen of Colorado. Plaintiff Pinkowski opened a Google+ account and has used it since the inception of the platform. Plaintiff also uses a Gmail account for her primary email. Through the opening and use of these accounts, Plaintiff Pinkowski has entrusted Google with her Personal Information for all relevant time periods.

B. Defendants

Defendant Google LLC ("Google"), is a Delaware corporation with its principal headquarters in Mountain View, California.

Defendant Alphabet Inc. ("Alphabet"), is a Delaware corporation with its principal headquarters in Mountain View, California. Alphabet is a public holding company formed in a corporate reorganization by Google. Through the corporate restructuring, Defendant Google is now a direct, wholly owned subsidiary of Defendant Alphabet.[1]

At all relevant times, Defendants were and are engaged in business in San Mateo County and throughout the United States of America.

FACTUAL BACKGROUND

A. Defendants Made Specific Representations to Users Regarding Defendants' Protection of Users' Personal Information

Google's Terms of Service make it clear that Google collects information from its users.[2] However, at all relevant times, Google has maintained a Privacy Policy that makes specific representations to Users regarding its protection and exposure of their Personal Information.[3]

[1] Google, *Form 8-K* filed with the U.S. Securities and Exchange Commission ("SEC") on August 10, 2015, https://www.sec.gov/Archives/edgar/data/1288776/000128877615000039/a20150810form8-k.htm (last visited December 11, 2018).

[2] Google, *Terms of Service* (October 25, 2017), https://policies.google.com/terms?hl=en&gl=ZZ (last visited December 11, 2018).

[3] Google, *Privacy Policy* (May 25, 2018), https://policies.google.com/privacy (last visited December 11, 2018).

The Google Privacy Policy specifically advises Users that: "When you use our services, you're ***trusting us*** with your information.[4] We understand this is a ***big responsibility*** and work hard to protect your information and put ***you*** in control." Further, Google represents that "We'll share Personal Information outside Google ***when we have your consent***."[5]

Other specific representations to Users in the Google Privacy Policy include:

1. "You have choices regarding the information we collect and how it's used."[6]
2. "We'll ask for your consent before using your information for a purpose that isn't covered in this Privacy Policy."[7]
3. "We'll ask for your ***explicit*** consent to share any sensitive personal information."[8]

And importantly for the Google+ Data Leaks, Google represents to its users they can "[c]ontrol whom you share information with through your account on Google+."[9]

Despite these representations, Google's lax approach to data security resulted in the Google+ Data Leaks affecting up to 53 million Google+ users over a period of at least 3 years.[10]

Likewise, Google has specifically disclosed that it owes a duty to Users to timely inform them of breaches involving private personal data, like the Personal Information exposed in the Google+ Data Leaks. On December 11, 2018, Google CEO Sundar Pichai was called to testify before the House Judiciary Committee on the various privacy and antitrust issues plaguing Google, including the Google+ Data Leaks.[11] During an exchange with Congressman Jerrold Nadler (D-NY), in a direct reference to the Google+ Data Leaks, Pichai admitted that Google

[4] *Id* (emphasis added).
[5] *Id* (emphasis added).
[6] *Id.*
[7] *Id.*
[8] *Id* (emphasis added).
[9] *Id.*
[10] The Wall Street Journal, *Google Exposed User Data, Feared Repercussions of Disclosing to Public* (October 8, 2018), *available at* https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194 (last visited December 11, 2018); The Wall Street Journal, *Google to Accelerate Closure of Google+ Social Network After Finding New Software Bug* (December 10, 2018), *available at* https://www.wsj.com/articles/google-to-accelerate-closure-of-google-social-network-1544465975 (last visited December 11, 2018).
[11] C-SPAN, *Google Data Collection* (December 11, 2018) *available at* https://www.c-span.org/video/?455607-1/google-ceo-sundar-pichai-testifies-data-privacy-bias-concerns (last visited December 18, 2018).

understood that it needed to notify impacted Users within ***72 hours*** of ascertaining who the Users are:

> **Jerrold Nadler (D-NY)**: According to media reports Google found evidence that – well, let me go to the other one first. Google found a bug in its Google Plus social media platform that could have potentially exposed the private data of up to half a million users without the consent to third-party developers. Google however did not disclose this bug until months later after it was revealed by a report in the Wall Street Journal. Yesterday, as I mentioned before, they found – you announced another bug. ***What legal obligations is the company under to disclose data exposures that do not involve sensitive financial information, but still involve private personal data, like users' name, age, email address or phone number***. . . .
>
> **Sundar Pichai (CEO – Google)**: Today, right now, if you've found a bug – you know, and you've ascertained – once you've done the investigation and you've ascertained the users who are eligible for notification, my understanding is **you have *72 hours***, and we both notify users as well as regulators in that timeframe.[12]

Despite Pichai's representations of Defendants' duty of timely disclosure, Defendants hid the First Data Leak from Users, the general public, and regulators for over ***7 months***.

B. Google's Inadequate Data Security Allowed for the First Data Leak Which Was Intentionally Concealed from the Public for Over Seven Months

On October 8, 2018, Defendants announced that they would be permanently shutting down the consumer functionality of Google+.[13] Within this announcement, Defendants disclosed that a "software glitch" had allowed outside application (i.e. "app") vendors access to private Google+ User profile data between 2015 and March 2018.[14]

Google+ Users may allow third party applications to access their private profile data. But a "glitch" or "bug" in the Application Program Interfaces ("API") allowed third-party applications to access the personal profile data of other Google+ Users within the authorizing User's circles

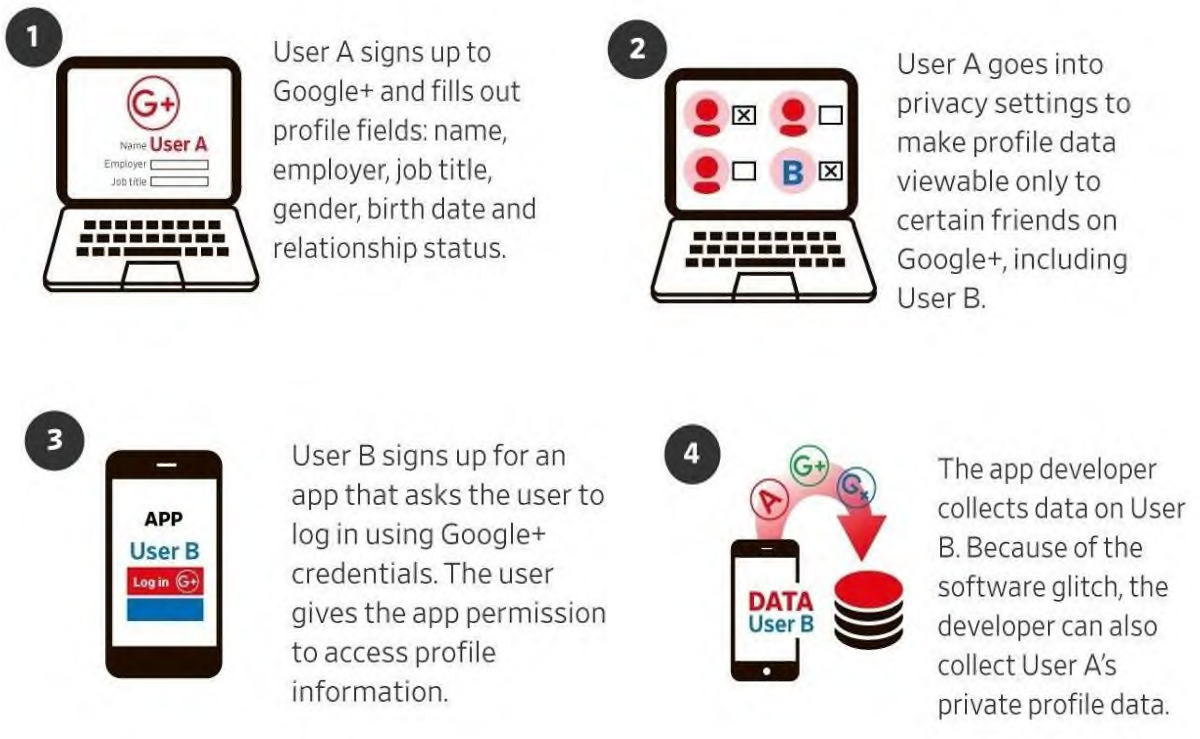
[12] *Id. at* 41:00.

[13] Google, *Project Strobe: Protecting your data, improving our third-party APIs, and sunsetting consumer Google+*, (October 8, 2018), *available at* https://www.blog.google/technology/safety-security/project-strobe/ (last visited December 11, 2018); *see also* The Wall Street Journal, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*, *supra* fn. 10.

[14] *Google, Project Strobe: Protecting your data, improving our third-party APIs, and sunsetting consumer Google+*, *supra* fn. 11.

without User consent. Google represented that this vulnerability could have potentially affected up to half a million Google users from 2015 and May 2018.[15]

In sum, the First Data Leak made it possible for third parties to access private Personal Information about Users who never had an opportunity to consent to such access. The access allowed through this "glitch" is shown in the following illustration:



Defendants have advised that at least 438 third-party applications may have used the API related to the First Data Leak and thereby had been allowed unauthorized access to certain Google+ users' Personal Information for nearly 3 years.[16]

When the First Data Leak was disclosed, it immediately drew comparisons to Facebook's leak of user information to Cambridge Analytica and other third-party application developers.[17]

[15] The Wall Street Journal, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*, *supra* fn. 10.

[16] *Google, Project Strobe: Protecting your data, improving our third-party APIs, and sunsetting consumer Google+*, *supra* fn. 11.

[17] The Wall Street Journal, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*, *supra* fn. 10. *See also* The Washington Post, *Facebook: 'Malicious actors' used its tools to discover identities and collect data on a massive global scale* (April 4, 2018), *available at* https://www.washingtonpost.com/news/the-

Given that Google+ was launched to challenge Facebook, the data security incidents suffered by Facebook users should have made Defendants more sensitive to the necessary protection of Google+ Users' data.

Instead, after discovering this vulnerability in the Google+ platform, Defendants kept silent for at least seven months, making a calculated decision to not inform Users that their Personal Information was compromised and allowing the unauthorized compromise of Users' Personal information and their exposure to risk of identity theft or worse to continue during that time.

Although Defendants claimed in the blog post announcing the First Data Leak that they "found no evidence that any developer was aware of this bug, or abusing the API" or "that any Profile data was misused," Defendants also represented that they only kept logs for two weeks.[18] Thus, based on Defendants' own admission that they can only account for whether the Google+ vulnerability had been exploited in the two weeks preceding its discovery, they have insufficient records to confirm whether and what data breaches had occurred during the three-year exposure period. As such, the full extent of the damage caused by Defendants' failure to provide adequate controls and protection for Users' Personal Information may never be known. Accordingly, the number of impacted Users, as well as the third-party applications that may have been able to exploit the Google+ vulnerability to access Users' Personal Information, was likely significantly more than what Google disclosed – 500,000 Users and 438 third-party applications.

Plaintiffs' gravest concerns proved true when Defendants announced the Second Data Leak just over two months later, which concerned similar-if-not-identical API, exposing the Personal Information of approximately 52.5 million Google+ Users – bringing the total potential exposure to 53 million Google+ Users.[19]

switch/wp/2018/04/04/facebook-said-the-personal-data-of-most-its-2-billion-users-has-been-collected-and-shared-with-outsiders/?utm_term=.61ae2fe14b0b (last visited December 11, 2018).

[18] *Google, Project Strobe: Protecting your data, improving our third-party APIs, and sunsetting consumer Google+*, *supra* fn. 11.

[19] The Wall Street Journal, *Google to Accelerate Closure of Google+ Social Network After Finding New Software Bug*, *supra* fn. 10.

Although Defendants have represented that the Second Data Leak only existed from November 7, 2018 through November 13, 2018, Defendants have provided few details and still intend to operate the clearly bug-ridden and unsecure Google+ platform until April 2019.[20]

This case involves the absolute and intentional disregard with which Defendants have chosen to treat the Personal Information of Users who have utilized their Google+ social media platform. While this Personal Information was supposed to be protected and shared only with expressed permissions, Defendants – without authorization – exposed that information to third parties through lax and non-existent data safety and security policies and protocols.

C. Defendants' Business Decision to Not Immediately Disclose the First Data Leak Put Their Interests Above That of Google+ Users and Exacerbated the Harm Caused

Equally troubling to the widespread and unknown impact of the First Data Leak is Defendants' intentional effort, approved by their upper management, to conceal the leak from the public and their victims.

When Defendants announced the First Data Leak, they shocked the public by revealing that they had discovered and "fixed" the security vulnerability in March 2018 – an astonishing seven months before the announcement.[21]

According to the Wall Street Journal, a Google internal memorandum prepared by its legal and policy staff and shared with its senior executives revealed that Google had hidden the security vulnerability for six months to avoid public scrutiny about its privacy practices.[22] According to that internal memorandum, Defendants' decision not to disclose the Google+ vulnerability was motivated by the fear that doing so would draw "immediate regulatory interest," bring Google "into the spotlight alongside or even instead of Facebook despite having stayed under the radar

[20] *Id. See also* Google, *Expediting changes to Google+* (December 10, 2018), *available at* https://www.blog.google/technology/safety-security/expediting-changes-google-plus/ (last visited December 11, 2018).

[21] *Google, Project Strobe: Protecting your data, improving our third-party APIs, and sunsetting consumer Google+*, *supra* fn. 11.

[22] The Wall Street Journal, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*, *supra* fn. 10.

throughout the Cambridge Analytica scandal," and "almost [guarantee that] Sundar [Pichai, Chief Executive Officer of Google,] will testify before Congress."[23]

Google's failure to adequately disclose the Google+ vulnerability for months on end has made the regulatory and congressional interest in the data breach even greater than if Google had simply disclosed it when it was discovered. The First Data Leak has directly led to recent Congressional calls for investigation, including questions regarding Google's compliance with the aforementioned FTC consent decree's requirements with respect to privacy settings and the protection of private information.[24]

An October 11, 2018 letter to Pichai from Commerce Committee Chairman John Thune (R-S.D.) detailed Google's culture of concealment and opacity, noting that:

> At the same time that Facebook was learning the important lesson that tech firms must be forthright with the public about privacy issues, Google apparently elected to withhold information about a relevant vulnerability for fear of public scrutiny. We are especially disappointed given that Google's chief privacy officer testified before the Senate Commerce Committee on the issue of privacy on September 26, 2018—just two weeks ago—and did not take the opportunity to provide information regarding this very relevant issue to the Committee.[25]

In addition, an October 11, 2018 letter to Pichai from Senate Judiciary Committee Chairman Chuck Grassley not only detailed the obvious similarities between the First Data Leak and Facebook's widely publicized Cambridge Analytica scandal, but also reprimanded Google for its refusal to participate in past hearings on data breaches when it had concealed knowledge of the First Data Leak:

> In March of this year, data privacy and social media was in the spotlight thanks to events surrounding Facebook and Cambridge Analytica. I convened a hearing with the CEO of Facebook on April 10, 2018, and according to his testimony, a feature in Facebook's application programming interface, or API, allowed third party

[23] *Id.*

[24] *Senator Blumenthal's Letter to FTC Chairman* (October 10, 2018), *available at* https://www.blumenthal.senate.gov/imo/media/doc/10.10.18%20-%20FTC%20-%20Google%20Plus%20Exposure.pdf (last visited December 11, 2018); *Senator Thune's Letter to Sundar Pichai* (October 11, 2018), *available at* https://www.commerce.senate.gov/public/_cache/files/4852b311-0953-4ac8-ac43-a91dde229cc1/E300DA0C7659678AE0AE37AEB9746200.thune-wicker-moran-letter-to-google-10.11.18.pdf (last visited December 11, 2018); *Senator Grassley's Letter to Sundar Pichai* (October 11, 2018), *available at* https://www.judiciary.senate.gov/imo/media/doc/2018-04-10%20CEG%20to%20Google%20-%20Data%20Privacy.pdf (last visited December 11, 2018).

[25] *Senator Thune's Letter to Sundar Pichai*, *supra* fn. 22.

> developers to pull information not just from users of an application, but also that user's friends, even if the friend had made their information private. . . .
> At the time, I invited you and the CEO of Twitter to participate in the hearing to discuss the future of data privacy in the social media industry. . . . ***Your office, however, declined to come before Congress and the American people, asserting that the problems surrounding Facebook and Cambridge Analytica did not involve Google***.
>
> Given your and Google's unwillingness to participate. I sent you a letter seeking information on Google's current data privacy policies, specifically as they relate to Google's third-party developer APIs. Your responses to my questions highlighted Google's application verification process, the continuous, monitoring of applications through machine learning, and the use of manual audits, all to ensure robust protection of user data.
>
> ***Despite your contention that Google did not have the same data protection failures as Facebook, it appears from recent reports that Google+ had an almost identical feature to Facebook, which allowed third party developers to access information from users as well as private information of those users' connections.*** Moreover, it appears that you were aware of this issue at the time I invited you to participate in the hearing and sent you the letter regarding Google's policies.[26]

Defendants thus chose to protect themselves from potential governmental inquiry rather than protect the Personal Information of Google+ users and advise them that their Personal Information had been exposed in the First Data Leak to unauthorized third parties.

Defendants withheld the information of the First Data Leak from Google+ users and the public until announcing it alongside their decision to shut down the Google+ service for consumers in August 2019 —approximately 10 months later.

At every turn, Defendants put their own business interests ahead of the privacy interests of Google+ users, causing harm to Plaintiffs and Class members.

The First Data Leak has caused significant harm to Plaintiffs and other Class members by allowing third-parties to access their Personal Information without their consent. This harm was exacerbated by Google's culture of concealment and opacity regarding its insufficient data protection policies and the resulting data breach.

[26] *Senator Grassley's Letter to Pichai*, *supra* fn. 22 (emphasis added).

Despite numerous lapses in and rebukes on its approach to data security, Google still lacks sufficient safeguards and protections for Users' Personal Information and has shown a conscious disregard for any transparency regarding the potential exposure of their personal information. This danger has already manifested in the Second Data Leak revealed by Defendants just months later. Thus, Plaintiffs and Class members' Personal Information remains at risk today and into the future, until Google is compelled to secure their Personal Information.

D. Defendants Failed to Properly Secure Google+ After the First Data Leak, Resulting in the Exposure of Even More Users' Personal Information in the Second Data Leak

Despite the increased attention from the First Data Leak in October 2018, Defendants continued to operate the Google+ service and collect Users' Personal Information, with no plans to shut the Google+ service down until August 2019.

Then, just ***nine weeks*** after their announcement of the First Data Leak, Defendants had to disclose that they had again improperly exposed Users' Personal Information to third-party application developers.

Specifically, on December 10, 2018, Defendants announced that they would be expediting their closure of Google+ due to the Second Data Leak, whereby the Personal Information of Users was, again, improperly exposed to third-party application developers.[27] This time, up to 52.5 million Users were impacted.[28] Defendants had permitted the Second Data Leak to persist from November 7, 2018 until November 13, 2018, when they allegedly identified and fixed vulnerabilities that had again permitted unauthorized third parties to access and aggregate Users' Personal Information.[29]

The Second Data Leak allowed third-party application developers to view profile information from Users, including, *inter alia*, a User's name, email address, occupation, work

[27] Google, *Expediting changes to Google+* (December 10, 2018), *available at* https://www.blog.google/technology/safety-security/expediting-changes-google-plus/ (last visited December 11, 2018).

[28] *Id*.

[29] Statt and Brandom, *Google will shut down Google+ four months early after second data leak* (December 10, 2018), *available at https://www.theverge.com/platform/amp/2018/12/10/18134541/google-plus-privacy-api-data-leakdevelopers* (last visited December 11, 2018).

history, age, relationship status, biography, gender, and birthday – even if the User's account was set to private.[30] Third-party developers were also able to improperly access Users' profile data that had been shared with a specific User, but was not shared publicly by the User.[31]

As a result of the Second Data Leak, Defendants announced their decision to accelerate the shut-down of the consumer functionality of Google+ from August 2019 to April 2019.[32]

E. Users' Personal Information Is an Increasingly Valuable Commodity

Personal information from social media, like the Personal Information encompassed in the Google+ Data Leaks, is incredibly valuable to companies like Google. In 2017 alone, Google's advertisement revenue – which is dependent on Google's ability to collect personal information about its users – amounted to nearly $95.4 billion.[33]

One study found that the average consumer in the U.S. can make $240 per year monetizing his or her personal data for digital advertising.[34] Another study in 2018 found that social media advertising revenue currently amounts to $67.97 billion, and that the average revenue per Internet user currently amounts to approximately $22.84.[35] Similarly, a 2016 study found that Google makes approximately $7.00 per monthly active user each quarter, or approximately $28.00 per user each year.[36]

Defendants' calculation of the average revenue each user generates is derived from an analysis of, *inter alia*, the content and information each user shares.[37] Thus, when Users signed up to join Google+, they were entering into a transaction – a value-for-value exchange – in which

[30] Google, *Expediting changes to Google*, *supra* fn. 25; Google, *Google+ API, List of Personal Information*, *available at* https://developers.google.com/+/web/api/rest/latest/people (last visited December 11, 2018). *See also* Statton and Brandom, *supra*, fn. 26.

[31] *Id.*

[32] Google, *Expediting changes to Google*, *supra* fn. 25.

[33] Alphabet, *Form 10-K* for the fiscal year ended December 31, 2017, filed with the SEC on February 6, 2018, at 28.

[34] Medium, *How Much is Your Data Worth? At Least $240 per Year. Likely Much More*, *available at* https://medium.com/wibson/how-much-is-your-data-worth-at-least-240-per-year-likely-much-more-984e250c2ffa (last visited December 11, 2018).

[35] Statista, *Social Media Advertising*, *available at* https://www.statista.com/outlook/220/100/social-media-advertising/worldwide#market-revenuePerInternetUser (last visited December 11, 2018).

[36] Ampere Analysis, *Facebook Closes the Gap on Google*, *available at* https://www.ampereanalysis.com/blog/fd5b6dc9-d76e-40a8-b8f2-e5ed15bc32bb (last visited December 11, 2018).

[37] See, *i.e.*, Google, *Google AdMob ARPU (metric)*, *available at* https://support.google.com/admob/answer/7374260?hl=en (discussing the metric of average revenue per user, or ABPU, that third-party application developers have access to when using Google's AdMob advertising platform).

they agreed to provide content and Personal Information that Defendants could use, subject to the Users' privacy restrictions. Because exclusive access to such content and information confers a competitive advantage, there is a "first user" value to the content and information. That value has now been lost due to the Google+ Data Leaks.

Additionally, the Personal Information compromised in the Google+ Data Leaks is highly valuable to identity thieves. The names, birthdates, hometowns, addresses, locations, interests, relationships, email addresses, photos, and videos, and other valuable personal information can all be used to gain access to a variety of existing accounts and websites.

Identity thieves can also use the Personal Information to harm Plaintiffs and the other Class members through embarrassment, blackmail, or harassment in person or online or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential identity theft report from 2008 states that:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[38]

[38] U.S. FTC, *The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan*, (April 2007), https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last visited December 11, 2018).

To put it into context, the 2013 Norton Report[39] – based on one of the largest consumer cybercrime studies ever conducted – estimated that the global price tag of cybercrime was around ***$113 billion*** at that time, with the average cost per victim being $298 dollars, as demonstrated in the chart below:

The problems associated with identity theft are exacerbated by the fact that many identity thieves will wait years before attempting to use the Personal Information they have obtained. Indeed, in order to protect themselves, Plaintiffs and the other Class members will need to remain vigilant against unauthorized data use for years and decades to come.

Once stolen, personal information can be used in a number of different ways. One of the most common ways is that it is offered for sale on the dark web, a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. Due to its hidden nature and the use of special applications to maintain anonymity, the dark web is a haven for all kinds of illicit activity, including the trafficking of stolen personal information

[39] Norton by Symantec, *2013 Norton Report, available at* https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf (last visited December 10, 2018).

captured via data breaches or hacks.[40] One 2018 study found that an individual's online identity is worth approximately $1,170 on the dark web.[41]

Once someone buys personal information, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

Personal information can also be used by scammers to target victims using phishing scams.[42] Phishing is when scammers use personal information they have obtained about victims to send fraudulent emails or texts, or copycat websites to get victims to share additional valuable personal information – such as account numbers, Social Security numbers, or login IDs and passwords.[43] Scammers use victims' information, including Personal Information, to steal the victims' money, identity, or both.[44] Scammers also use phishing emails to get access to a victim's computer or network, then install programs like ransomware that can lock a victim out of important files on their computer.[45] According to one Federal Bureau of Investigation study, scammers collected more than $676 million in 2017 alone through two types of phishing scams: "Business Email Compromise" and "Email Account Compromise."[46]

Due to Defendants' conduct described herein, Plaintiffs and the other Class members have a greater risk of identity theft, manipulation, fraud, scams, and/or targeted unwanted and unnecessary advertising, including inappropriate communications. Additionally, Plaintiffs and the other Class members now face additional security risks such as phishing attempts, efforts by

[40] Experian, *What is the Dark Web?* (April 8, 2018), *available at* https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last visited December 10, 2018). *See also* Brian Hamrick, *The dark web: A trip into the underbelly of the internet*, WLWT News (Feb. 9, 2017), http://www.wlwt.com/article/the-dark-web-a-trip-into-the-underbelly-of-the-internet/8698419 (last visited December 10, 2018).

[41] TOP10VPN, Dark Web Market Price Index (US Edition) (February 27, 2018), *available at* https://www.top10vpn.com/privacy-central/privacy/dark-web-market-price-index-feb-2018-us/ (last visited December 10, 2018).

[42] U.S. FTC, *Phishing* (July 2017), *available at* https://www.consumer.ftc.gov/articles/0003-phishing (last visited December 12, 2018).

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] U.S. Federal Bureau of Investigation, *2017 Internet Crime Report*, *available at* https://pdf.ic3.gov/2017_IC3Report.pdf (last visited December 12, 2018).

hackers trying to access or log in to their online accounts, friend requests from trolls or cloned or imposter accounts, and/or other interference with their online accounts. Plaintiffs and the other Class members are subjected to a heightened risk of such predatory conduct due to Defendants' failure to secure their Personal Information, including the sale of their content and Personal Information on the dark web and other illicit databases.

F. Google Has A Long History of Improper Data Practices

Google has been on notice of deficiencies regarding its policies involving the retention of User data since at least 2010. The FTC specifically found that Google used deceptive tactics and violated its own privacy promises to consumers when it launched its first social network product, Google Buzz, in 2010.

As a result of such deficiencies, Google agreed to a proposed settlement in March 2011, which contained a consent decree under which the FTC barred Google from misrepresenting the privacy of personal information or the extent to which consumers may exercise control over the collection, use, or exposure of their covered personal information.[47] The FTC also required Google to establish a "comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information." Included in this privacy program was the "regular testing or monitoring of the effectiveness of those privacy controls and procedures," which would be audited by an independent third-party professional.[48]

Less than a year after entering into the FTC consent decree, Google violated it – becoming one of the rare companies in the country that has violated an FTC consent decree – and paid a record fine for its circumvention of privacy protections in the web browser Safari.[49] In discussing

[47] U.S. FTC, *In the Matter of GOOGLE INC., a corporation* (October 13, 2011), Docket No. C-4436, *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf (last visited December 11, 2018).

[48] *Id.*

[49] U.S. FTC, *Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser* (August 9, 2012), *available at* https://www.ftc.gov/news-events/press-

the settlement, Jon Leibowitz, Chairman of the FTC, said, "The record setting penalty in this matter sends a clear message to all companies under an FTC privacy order. No matter how big or small, all companies must abide by FTC orders against them and keep their privacy promises to consumers, or they will end up paying many times what it would have cost to comply in the first place."[50]

CLASS ACTION ALLEGATIONS

Pursuant to Federal Rules of Civil Procedure ("Rules" or "Rule") 23(b)(2), (b)(3), and (c)(4), Plaintiffs, individually and on behalf of all others similarly situated, bring this lawsuit on behalf of themselves and as a class action on behalf of the following Class:

> All persons in the United States who registered for Google+ accounts and whose Personal Information was accessed, compromised, or obtained from Google by third-party applications without authorization or in excess of authorization as a result of the 2018 Data Leaks.

Excluded from the Class are Defendants and any entities in which Defendants or their subsidiaries or affiliates have a controlling interest, as well as Defendants' officers, agents, and employees. Also excluded from the Class are the judge assigned to this action, members of the judge's staff, and any member of the judge's immediate family. Plaintiffs reserve the right to amend the Class definitions if discovery and further investigation reveal that any definitions should be expanded or otherwise modified.

Numerosity: The members of the Class are so numerous that joinder of all members of the Class would be impracticable. Defendants have indicated that at least 500,000 people had their Google+ accounts compromised as a result of the First Data Leak, and as many as 52,500,000 people had their Google+ accounts compromised as a result of the Second Data Leak. The identity of these Google+ users can be determined through records and documents maintained by Defendants.

releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented (last visited December 11, 2018).

[50] *Id.*

Commonality and Predominance: This action involves common questions of law or fact, which predominate over any questions affecting individual Class members, including:

i. Whether Defendants represented to Plaintiffs and the Class that they would safeguard Class members' Personal Information;

ii. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

iii. Whether Defendants breached a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

iv. Whether third parties improperly obtained Plaintiffs and Class members' Personal Information without authorization or in excess of any authorization;

v. Whether Defendants were aware of other third parties' collection of Plaintiffs and Class members' Personal Information without authorization or in excess of any authorization;

vi. Whether Defendants knew about the First Data Leak before it was announced to the public and whether Defendants failed to timely notify the public of the First Data Leak;

vii. Whether Defendants knew about the Second Data Leak before it was announced to the public and whether Defendants failed to timely notify the public of the Second Data Leak;

viii. Whether Defendants' conduct violated Cal. Civ. Code § 1750, *et seq.*;

ix. Whether Defendants' conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq.*;

x. Whether Defendants' conduct violated the Consumer Records Act, Cal. Civ. Code § 1798.80 *et seq.*;

xi. Whether Defendants' conduct violated § 5 of the FTC Act, 15 U.S.C. § 45, *et seq.*;

xii. Whether Plaintiffs and the Class are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and

xiii. Whether Plaintiffs and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the Class members. Similar or identical

statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

Google's choice-of-law provision is further indication of the common questions of law. Google's Terms of Service provide, in relevant part, that "you agree that the laws of California, U.S.A., excluding California's choice of law rules, will apply to any disputes arising out of or relating to these terms or the Services."

Typicality: Plaintiffs' claims are typical of the claims of the other members of the class because, among other things, Plaintiffs and the other Class members were injured through the substantially uniform misconduct by Defendants. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of other Class members arise from the same operative facts and are based on the same legal theories.

Adequacy of Representation: Plaintiffs are adequate representatives of the classes because their interests do not conflict with the interests of the other Class members they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and they will prosecute this action vigorously. The Class members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

Superiority: A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other members of their respective classes are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class members to individually seek redress for Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments, and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties

and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

Further, Defendants has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the members of the Class as a whole is appropriate under Rule 23(b)(2).

Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Class members' Personal Information was improperly obtained by third parties;

b. Whether (and when) Defendants knew about any security vulnerabilities that led to the First Data Leak before they were announced to the public and whether Defendants failed to timely notify the public of those vulnerabilities and the First Data Leak;

c. Whether (and when) Defendants knew about any security vulnerabilities that led to the Second Data Leak before they were announced to the public and whether Defendants failed to timely notify the public of those vulnerabilities and the Second Data Leak;

d. Whether Defendants' conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq.*;

e. Whether Defendants' representations that they would secure and protect the Personal Information of Plaintiffs and the other members of the Class were facts that reasonable persons could be expected to rely upon when deciding whether to use Defendants' services;

f. Whether Defendants misrepresented the safety of their many systems and services, specifically the security thereof, and their ability to safely store Plaintiffs' and the other Class members' Personal Information;

g. Whether Defendants concealed crucial information about their inadequate data security measures from Plaintiffs and the Class;

h. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

i. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and the other Class members' Personal Information secure and prevent the unauthorized disclosure of that information;

j. Whether Defendants failed to "implement and maintain reasonable security procedures and practices" for Plaintiffs' and the other Class members' Personal Information in violation of § 5 of the FTC Act;

k. Whether Defendants failed to provide timely notice of the First Data Leak in violation of California Civil Code § 1798.82;

l. Whether Defendants failed to provide timely notice of the Second Data Leak in violation of California Civil Code § 1798.82;

m. Whether Defendants' conduct violated Cal. Bus. & Prof. Code § 22575, *et seq.*;

n. Whether Defendants owed a duty to Plaintiffs and the Class to safeguard their Personal Information and to implement adequate data security measures;

o. Whether Defendants breached that duty;

p. Whether Defendants failed to adhere to their posted privacy policy concerning the care they would take to safeguard Plaintiffs' and the other Class members' Personal Information in violation of California Business and Professions Code § 22576;

q. Whether Defendants negligently and materially failed to adhere to their posted privacy policy with respect to the extent of their disclosure of users' data, in violation of California Business and Professions Code § 22576;

r. Whether such representations were false with regard to storing and safeguarding Class and Class members' Personal Information; and

s. Whether such representations were material with regard to storing and safeguarding Class members' Personal Information.

First Claim for Relief

Violation of California's Unfair Competition Law ("UCL") – Unlawful Business Practice (Cal. Bus. & Prof. Code § 17200, et seq.)

Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

Defendants' choice-of-law provision establishes that California law applies to Plaintiffs' and the other Class members' claims.

By reason of the conduct alleged herein, Defendants engaged in unlawful practices within the meaning of the UCL. The conduct alleged herein is a "business practice" within the meaning of the UCL.

Google represented that it would not disclose Google+ users' Personal Information without consent and/or notice. Google further represented that it would utilize sufficient data security protocols and mechanisms to protect Google+ users' Personal Information.

Defendants failed to abide by these representations. Defendants did not prevent the improper disclosure of Plaintiffs' and the Class's Personal Information.

Defendants stored the Personal Information of Plaintiffs and the members of their respective Classes in Defendants' electronic and consumer information databases. Defendants falsely represented to Plaintiffs and the other members of the Classes that the Personal Information databases were secure and that their Personal Information would remain private. Defendants knew or should have known they did not employ reasonable, industry standard, and appropriate security measures that complied "with federal regulations" and that would have kept Plaintiffs' and the other Class members' Personal Information secure and prevented the loss or misuse of such Personal Information.

Even without these misrepresentations, Plaintiffs and the other Class members were entitled to assume, and did assume, that Defendants would take appropriate measures to keep their Personal Information safe. Defendants did not disclose at any time that Plaintiffs' Personal Information was accessible to third party application vendors because Defendants' data security measures were inadequate, even though Defendants were the only ones in possession of that material information, which they had a duty to disclose. Defendants violated the UCL by misrepresenting, both by affirmative conduct and by omission, the strength of the security of their many systems and services, and their ability to honor the disclosure authorizations established by Plaintiffs and the other Class members for their Personal Information.

Defendants also violated the UCL by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and failing to comply with their

own posted privacy policies. If Defendants had complied with these legal requirements, Plaintiffs and the other Class members would not have suffered the damages described herein.

Defendants' acts, omissions, and misrepresentations, as alleged herein, were unlawful and in violation of, *inter alia*, Section 5(a) of the FTC Act and 15 U.S.C. § 45(a), Cal. Bus. & Prof. Code § 22576 (as a result of Google failing to comply with its own posted privacy policies).

Plaintiffs and the other Class members suffered injury in fact and lost money or property as the result of Defendants' unlawful business practices. In particular, Plaintiffs' and the other Class members' Personal Information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that such information is of tangible value.

As a result of Defendants' unlawful business practices, which are violations of the UCL, Plaintiffs and the other Class members are entitled to restitution, disgorgement of wrongfully obtained profits, and injunctive relief.

Second Claim for Relief

Violation of California's UCL – Unfair Business Practice
(Cal. Bus. & Prof. Code § 17200, *et seq*.)

Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

Defendants' choice-of-law provision establishes that California law applies to Plaintiffs' and the other Class members' claims.

By reason of the conduct alleged herein, Defendants engaged in unfair "business practices" within the meaning of the UCL.

Defendants stored the Personal Information of Plaintiffs and the members of their respective Classes in their electronic and consumer information databases. Defendants represented to Plaintiffs and the other members of the Class that their Personal Information databases were secure and that such Personal Information would remain private and be disclosed only with expressed authorization. Defendants engaged in unfair acts and business practices by

representing that they would require expressed consent and authorization from Plaintiffs and the other Class members prior to the disclosure of Personal Information to third parties.

Even without these misrepresentations, Plaintiffs and the other Class members were entitled to, and did, assume Defendants would take appropriate measures to keep their Personal Information safe. Defendants did not disclose at any time that Plaintiffs' Personal Information was vulnerable to unauthorized disclosure because Defendants' data security measures were inadequate, even though Defendants were in sole possession of that material information, which they had a duty to disclose.

Defendants knew or should have known they did not employ reasonable measures that would have kept Plaintiffs' and the other Class members' Personal Information secure from unauthorized disclosure.

Defendants engaged in unfair acts and business practices by representing that they would not disclose this Personal Information without authorization and/or by obtaining that Personal Information without authorization. Not only did Defendants also violate their commitment to maintain the confidentiality and security of the Personal Information of Plaintiffs and their respective Classes, but they failed to comply with their own stated policies and applicable laws, regulations, and industry standards relating to data security.

Defendants engaged in unfair business practices under the "balancing test." The harm caused by Defendants' actions and omissions, as described in detail *supra*, greatly outweigh any perceived utility. Indeed, Defendants' failure to follow basic data security protocols and misrepresentations to consumers about Defendants' data security cannot be said to have had any utility at all.

Defendants engaged in unfair business practices under the "tethering test." Defendants' actions and omissions, as described in detail *supra*, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that ... all individuals have a right of privacy in information pertaining to them.... The increasing use of computers ... has greatly magnified the potential risk to individual privacy that can occur from the maintenance of Personal Information."); Cal. Bus. & Prof. Code

§ 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendants' acts and omissions, and the injuries caused by them, are thus "comparable to or the same as a violation of the law …" *Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.* (1999) 20 Cal.4th 163, 187.

Defendants engaged in unfair business practices under the "FTC test." The harm caused by Defendants' actions and omissions, as described in detail *supra*, is substantial in that it affects up to 53 million Class members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Class members' Personal Information to third parties without their consent, diminution in value of their Personal Information, and consequential out-of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Class members' Personal Information remains in Defendants' possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendants' actions and omissions violated, *inter alia*, Section 5(a) of the FTC Act, 15 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham Worldwide Corp*., 10 F. Supp. 3d 602, 613 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015); *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure Personal Information collected violated § 5(a) of FTC Act); *In re BJ's Wholesale Club, Inc*., FTC Docket No. C-4148, FTC File No. 042-3160 (Sept. 20, 2005) (same); *In re CardSystems Solutions, Inc*., FTC Docket No. C-4168, FTC File No. 052-3148 (Sept. 5, 2006) (same); *see also United States v. ChoicePoint, Inc*., Civil Action No. 1:06-cv-0198-JTC (N.D. Ga. Oct. 14, 2009) ("failure to establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security. confidentiality, and integrity of Personal Information collected from or about consumers" violates § 5(a) of FTC Act); 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.").

Plaintiffs and the other Class members suffered injury in fact and lost money or property as the result of Defendants' unfair business practices. In addition, their Personal Information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value.

As a result of Defendants' unfair business practices, which are violations of the UCL, Plaintiffs and the other Class members are entitled to restitution, disgorgement of wrongfully obtained profits, and injunctive relief.

Third Claim for Relief

Violation of California's UCL – Fraudulent/Deceptive Business Practice (Cal. Bus. & Prof. Code § 17200, *et seq*.)

Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

Defendants' choice-of-law provision establishes that California law applies to Plaintiffs' and the other Class members' claims.

Defendants engaged in fraudulent and deceptive acts and practices with regard to the services they provided to the Class by representing and advertising that (1) they would maintain adequate data privacy and security practices and procedures to safeguard Class members' Personal Information from unauthorized disclosure, release, data breaches, and theft; and (2) they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class members' Personal Information. These representations were likely to deceive members of the public, including Plaintiffs and the other Class members, into believing their Personal Information was securely stored – when it was not – and that Defendants were complying with relevant law – when they were not.

Defendants engaged in fraudulent and deceptive acts and practices with regard to the services provided to the Class by omitting, suppressing, and concealing the material fact that the privacy and security protections for Class members' Personal Information was woefully inadequate. At the time that Class members were using Defendants' services, Defendants failed to disclose to Class members that their data security systems failed to meet legal and industry

standards for the protection of Class members' Personal Information. These representations likely deceived members of the public, including Plaintiffs and the Class, into believing that their Personal Information was securely stored – when it was not – and that Defendants were complying with relevant law and industry standards – when they were not.

As a direct and proximate result of Defendants' deceptive practices and acts, Plaintiffs and the Class were injured and lost money or property, including but not limited to the loss of their legally protected interest in the confidentiality and privacy of their Personal Information, as well as the additional losses described *supra*.

Defendants knew or should have known that their computer systems and data security practices were inadequately safeguarding Class members' Personal Information and that the risk of a data breach or theft was very high.

Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Class.

Class members seek relief under Cal. Bus. & Prof. Code § 17200, *et. seq*., including, but not limited to, restitution to Plaintiffs and the Class of money or property that Defendants may have acquired by means of their fraudulent and deceptive business practices, restitutionary disgorgement of all profits accruing to Defendants because of their fraudulent and deceptive business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

Fourth Claim for Relief

Negligence

Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

Defendants owed a duty to Plaintiffs and the Class to exercise reasonable care in safeguarding and protecting their Personal Information and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties.

Defendants knew that the Personal Information of Plaintiffs and the Class was personal and sensitive information that is valuable to identity thieves and other criminals. Defendants also knew of the serious harms that could occur if the Personal Information of Plaintiffs and the Class was wrongfully disclosed, that disclosure was not fixed, and/or Plaintiffs and the Class were not told about the disclosure in a timely manner.

By being entrusted by Plaintiffs and the Class to safeguard their Personal Information, Defendants had a special relationship with Plaintiffs and the Class. Plaintiffs and the Class signed up for Defendants' services and agreed to provide their Personal Information with the understanding that Defendants would take appropriate measures to protect it and would inform Plaintiffs and the Class of any breaches or other security concerns that might call for action by Plaintiffs and the Class. But, Defendants did not. Defendants not only knew that their data security was inadequate, they also knew that they did not have the tools to detect and document intrusions or exfiltration of Plaintiffs' and the Class' Personal Information.

Defendants breached their duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class members' Personal Information by failing to adopt, implement, and maintain adequate security measures to safeguard that information and prevent unauthorized disclosure of Plaintiffs' and the other Class members' Personal Information.

Defendants also breached their duty to timely disclose that Plaintiffs' and the other class members' Personal Information had been, or was reasonably believed to have been, improperly obtained.

But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and the Class, their Personal Information would not have been compromised, stolen, and viewed by unauthorized persons.

Defendants' negligence was a direct and legal cause of the theft of the Personal Information of Plaintiffs and the Class and all resulting damages.

The injury and harm suffered by Plaintiffs and the other Class members was the reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other class members' Personal Information. Defendants knew

their systems and technologies for processing and securing the Personal Information of Plaintiffs and the Class had numerous security vulnerabilities.

As a result of this misconduct by Defendants, the Personal Information of Plaintiffs and the Class was compromised – placing them at a greater risk of identity theft and subjecting them to identity theft – and was disclosed to third parties without their consent.

As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and the other Class members have suffered injury and are entitled to appropriate relief, including injunctive relief and damages.

Fifth Claim for Relief

Invasion of Privacy

Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

Defendants' choice-of-law provision establishes that California law applies to Plaintiffs' and all Class members' claims.

The California Constitution expressly provides for a right to privacy. Cal. Const. Art. I, Sec. 1.

Google's terms of use for all times relevant to this matter provided that users' Personal Information would not be released to third parties without express consent.

Absent their express consent, Plaintiffs and the other Class members used Google+ under the impression that Personal Information was safeguarded and would not be provided to, or stolen by, third parties.

Plaintiffs and the other Class members had an interest in the protection and non-dissemination of their Personal Information that Defendants electronically stored, including the right not to have that Personal Information stolen and used for profit.

Absent the express consent of Google+ users, Defendants intentionally intruded on Plaintiffs' and the other Class members' private life, seclusion, and solitude, which is protected under the California constitution as well as common law.

Defendants' wrongful conduct constitutes breach of the social norms underpinning the constitutionally-protected right to privacy.

Defendants' wrongful conduct harmed Plaintiffs and the other Class members.

As a direct and proximate result of Defendants' wrongful conduct, Plaintiffs and the other Class members have suffered injury and are entitled to appropriate relief, including injunctive relief and damages.

Sixth Claim for Relief

Breach of Confidence

Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

This claim is asserted against Defendants for breach of confidence concerning the Personal Information that Plaintiffs and the other Class members provided to Defendants in confidence.

At all times during Plaintiffs' and the other Class members' interactions with Defendants, Defendants were fully aware of the confidential nature of the Personal Information that Plaintiffs and Class members shared with Defendants.

As alleged herein and above, Defendants' relationship with Plaintiffs and Class members was governed by Google's Terms of Service and the expectation that Plaintiffs' and Class members' Personal Information would be collected, stored, and protected in confidence by Defendants, and not disclosed to unauthorized third parties.

Plaintiffs and the other Class members provided their respective Personal Information to Defendants with the explicit and implicit understanding that Defendants would protect and not permit that Personal Information to be disseminated to any unauthorized third parties.

Defendants voluntarily received in confidence Plaintiffs' and the other Class members' Personal Information with the understanding that that Personal Information would not be disclosed or disseminated to the public or any unauthorized third parties.

Due to Defendants' failure to prevent, detect, and stop the 2018 Data Leaks from occurring, Plaintiffs' and the other Class members' Personal Information was disclosed and

misappropriated to unauthorized third parties beyond their confidence and without their express permission.

As a direct and proximate cause of Defendants' actions and inactions, Plaintiffs and the other Class members have suffered damages.

But for Defendants' disclosure of Personal Information in violation of the parties' understanding that it would be held in confidence, Plaintiffs and the other Class members' Personal Information would not have been compromised, stolen, and viewed by unauthorized persons. Defendants' disclosure was a direct and legal cause of the theft of Plaintiffs' and the other Class members' Personal Information, as well as the resulting damages.

The injury and harm Plaintiffs and the other Class members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiffs' and Class members' Personal Information. Defendants knew their computer systems and technologies for accepting and securing Plaintiffs' and Class members' Personal Information had numerous security vulnerabilities, but Defendants continued to collect, store, and maintain Plaintiffs' and Class members' Personal Information without fixing the vulnerabilities, even after the First Data Leak.

As a result of Defendants' misconduct, Plaintiffs' and the other Class members' Personal Information was compromised – placing them at a greater risk of identity theft and subjecting them to identity theft and fraud – and disclosed to unauthorized third parties without their consent. Plaintiffs and the other Class members also suffered diminution in value of their Personal Information in that it became easily available to hackers on the dark web. Plaintiffs and the other Class members have also suffered consequential out-of-pocket losses for procuring credit freezes or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

Seventh Claim for Relief

Deceit by Concealment or Omission
(Cal. Civil Code §§ 1709, 1710)

Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

Defendants' choice-of-law provision establishes that California law applies to Plaintiffs' and the other Class members' claims.

As alleged above, Defendants knew that their data security measures were grossly inadequate by, at the absolute latest, March 2018. At that time, Defendants were on notice of the software glitch in Google+ that gave outside developers potential access to private Google+ User profile data – facts that Defendants should have already known given their previous exposures and security problems.

In response to all of these facts, Defendants chose to do nothing to protect Plaintiffs and the Class or warn them about the security problems. Instead, Defendants chose to conceal the breach in order to avoid public backlash and a Congressional inquiry. Defendants' actions thereby allowed third-party application developers to improperly collect the Personal Information of up to 53 million Google+ users

Defendants had an obligation to disclose to all Class members that their Google account(s) and Personal Information were potentially compromised by the data breach.

Defendants made no such disclosure following the First Data Leak. Instead, Defendants willfully deceived Plaintiffs and the Class by concealing the true facts concerning their poor data security even though they were obligated to, and had a duty to, disclose those facts.

Had Defendants disclosed the true facts about their poor data security, Plaintiffs and the Class would have taken measures to protect themselves. Plaintiffs and the Class justifiably relied on Defendants to provide accurate and complete information about Defendants' data security, which Defendants failed to do.

Independent of any representations made by Defendants, Plaintiffs and the Class justifiably relied on Defendants to provide a service with at least minimally adequate security measures and to disclose facts undermining that reliance.

Rather than disclosing to Plaintiffs and the Class that the Google+ platform had been compromised by the breach and that Personal Information had been improperly exposed in the First Data Leak, Defendants continued with business as usual, concealing information relating to the inadequacy of their security measures from Plaintiffs and the Class.

While Defendants represented that they had fixed the vulnerability after the First Data Leak, they continued to conceal information relating to the inadequacy of their security measures, which resulted in the Second Data Leak.

These actions are "deceit" under Cal. Civil Code § 1710 in that they are the suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact.

As a result of this deceit by Defendants, they are liable under Cal. Civil Code § 1709 for "any damage which [Plaintiffs and the Class] thereby suffer[]."

As a result of this deceit by Defendants, the Personal Information of Plaintiffs and the Class were compromised, and their Personal Information was disclosed to third parties without their consent. Plaintiffs and the other Class members also suffered diminution in value of their Personal Information. Plaintiffs and the Class have also suffered consequential out-of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

Defendants' deceit, as alleged herein, is fraud under Civil Code § 3294(c)(3) in that it was a deceit or concealment of a material fact known to Defendants conducted with the intent on the part of Defendants of depriving Plaintiffs and the Class of "legal rights or otherwise causing injury." As a result, Plaintiffs and the Class are entitled to punitive damages against Defendants under Civil Code § 3294(a).

Eighth Claim for Relief

Breach of Contract

Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

At all relevant times, Defendants and Plaintiffs mutually assented to, and therefore were bound by the version of Google's Terms of Service and Privacy Policy (collectively, the "Contracts") that was operative at the time each of the Plaintiffs and other Class members joined Google+.

Throughout the Class Period, Defendants affirmatively stated in the Contracts that they would not disclose Google+ users' Personal Information without consent and/or notice. Defendants further represented in the Contracts that they would utilize sufficient data security protocols and mechanisms to protect Google+ users' Personal Information.

None of the Contracts informed and obtained Users' meaningful and lawfully-obtained consent to share their content and information with third parties without their consent, or disclosed that such information would be shared if their contacts entered into an agreement which permitted third parties to collect their contacts' information.

Thus, per the provision above, the Contracts did not authorize Defendants to share Plaintiffs' and the other Class members' Personal Information with third parties without their consent.

Plaintiffs and the other Class members fully performed their obligations under the Contracts.

Defendants breached the Contracts they entered into with Plaintiffs and the other Class members by failing to safeguard and protect their Personal Information, and improperly allowing third parties to access their Personal Information without their consent.

As a direct and proximate result of Google's breaches of the Contracts between Defendants and Plaintiffs and the other Class members, Plaintiffs and the other Class members sustained actual losses and damages, as described in detail *supra*. Plaintiffs and the other Class members suffered injury-in-fact and lost money or property. In addition, Plaintiffs and the other Class members' Personal Information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value.

Ninth Claim for Relief

Breach of Implied Covenant of Good Faith and Fair Dealing (In the Alternative)

Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein. This claim is pleaded in the alternative to the claim for breach of contract.

Defendants' choice-of-law provision establishes that California law applies to Plaintiffs' and the other Class members' claims.

Under California law, there is in every contract or agreement an implied promise of good faith and fair dealing. Such a duty is read into contracts and functions as a supplement to the express contractual covenants, in order to prevent a transgressing party from engaging in conduct which (while not technically transgressing the express covenants) frustrates the other party's rights to the benefit of the contract. Thus, any claim on the part of Defendants that they were technically permitted to allow the collection and transmittal of Plaintiffs' and the other Class members' Personal Information must be read in the context of, and give way to, their rights to the benefit of the contract, including the terms strictly delimiting such activity.

Defendants made specific representations to Plaintiffs and the other Class members regarding Defendants' protection of Users' Personal Information in their Privacy Policy that was operative at the time each of the Plaintiffs and other Class members joined Google+.

A covenant of good faith and fair dealing attaches to Defendants' Privacy Policy.

Throughout the Class Period, Defendants affirmatively stated in the Privacy Policy that they would not disclose Google+ users' Personal Information without their consent and/or notice. Defendants further represented in the Privacy Policy that they would utilize sufficient data security protocols and mechanisms to protect Google+ users' Personal Information.

Plaintiffs and the other Class members fully performed their obligations under the contractual provisions in the Privacy Policy.

Under the terms of the Privacy Policy, Plaintiffs and the other Class members were entitled to receive the benefits promised to them by Defendants, including that Defendants would

protect their Personal Information, would not disclose their Personal Information to third parties without their consent, and would keep their Personal Information secure.

Defendants were uniquely able to control the rights of their Users, including Plaintiffs and the other Class members, concerning their privacy, ownership, and control of their content and information, and whether that content and information would be provided to third parties without their consent.

Defendants surreptitiously took measures to frustrate and undercut Plaintiffs' and the other Class members' contractual rights concerning their privacy, ownership, and control over their Personal Information, and whether their content and information would be provided to third parties without their consent. By doing so, Defendants deprived Plaintiffs and the other Class members of the benefits under their contracts with Defendants, including the Privacy Policy.

As a direct and proximate result of Defendants' breaches of their duty of good faith and fair dealing, Plaintiffs and the other Class members sustained actual losses and damages, as described in detail *supra*. Plaintiffs and the other Class members suffered injury-in-fact and lost money or property. In addition, their Personal Information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other Class members, respectfully request that this Court enter an Order:

a. Certifying the United States Class, appointing Plaintiffs as Class Representatives, and appointing the law firms of Franklin D. Azar & Associates and Morgan & Morgan Complex Litigation Group as Class Counsel;

b. Finding that Defendants' conduct was negligent, deceptive, unfair, and unlawful as alleged herein;

c. Enjoining Defendants from engaging in further negligent, deceptive, unfair, and unlawful business practices as alleged herein;

d. Awarding Plaintiffs and the other Class members actual, compensatory, and consequential damages;

e. Awarding Plaintiffs and the other Class members statutory damages and penalties, as allowed by law;

f. Awarding Plaintiffs and the other Class members restitution and disgorgement;

g. Requiring Defendants to provide appropriate credit monitoring services to Plaintiffs and the other class members;

h. Awarding Plaintiffs and the other Class members punitive damages;

i. Awarding Plaintiffs and the other Class members pre-judgment and post-judgment interest;

j. Awarding Plaintiffs and the other Class members reasonable attorneys' fees costs and expenses, and;

k. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Consolidated Class Action Complaint so triable.

Dated: February 6, 2019

/s/ Ivy T. Ngo

Ivy T. Ngo (249860)
Franklin D. Azar & Associates, P.C.
Counsel for Plaintiffs Olson and Pinkowski

John A. Yanchunis (*pro hac vice*)
Jonathan B. Cohen (*pro hac vice*)
Ryan J. McGee (*pro hac vice*)
Morgan & Morgan
Complex Litigation Group

Clayeo C. Arnold (65070)
Clayeo C. Arnold, P.C.
Counsel for Plaintiffs Matic and Harris